SECURITY REPORT

HYPR | VansonBourne

Spotlight Report:

Workplace Identity Security Trends and Challenges to Watch in 2024

Introduction

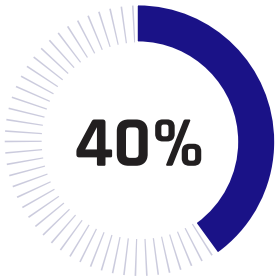
Identity underpins almost every aspect of today's workplace. Jobs cannot be performed without secure system access that relies on legitimate digital credentials tied to verified employees.

Identity and access management (IAM) has always had to strike a careful balance between security vs. convenience, user restrictiveness vs. productivity. The increasing interconnectedness and decentralization of systems, along with the explosion in the number of digital identities, is putting an unprecedented strain on organizations' IAM processes. Threat actors, quick to exploit any security gaps, are stepping up their attacks on identity systems. The result is a marked escalation in the number and severity of identity-related breaches .

With this in mind, HYPR set out to understand the identity security landscape and challenges facing organizations today. Independent research firm Vanson Bourne surveyed IT security leaders across the United States with deep knowledge and/or responsibility for IAM security, from organizations with more than 1,000 employees. They shared their insights on current practices, pain points and future plans to strengthen their organizations' identity security posture.

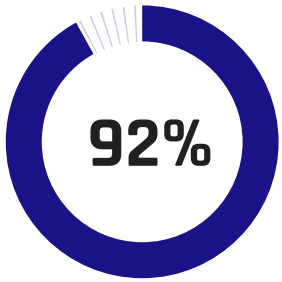
The research finds that many struggle to build an integrated and comprehensive identity security strategy, relying on disconnected tools and practices that create inefficiencies and leave organizations seriously vulnerable to attacks and breaches.

Key Findings



of organizations name identity verification as a top identity challenge

of employees' identities are monitored on a daily basis for risk or indications of compromise



of organizations have been the victim of identity fraud in the last 12 months

$4.33 million average cost of identity fraud per organization over the last 12 months

The Identity Threat Landscape in 2024

The Rise of Generative-AI Attacks

While generative AI has been a boon to many industries, it's also put even more power in the hands of cybercriminals. They can exploit zero days faster and create infinite new variants of malware to evade antivirus scanners. With generative AI, hackers can scrape social media profiles, company news and other relevant information to tailor every single phishing message. They can create deepfakes that are convincing enough to successfully manipulate others into divulging sensitive information or resetting credentials.

Targeting Identity Processes

Whether with or without generative AI, social engineering attacks on identity are skyrocketing, exposing massive weaknesses in the identity security fabric. 2023 saw a near-continuous string of breaches of identity systems and processes — current approaches simply cannot keep up with threats. Even with multi-factor authentication (MFA) in place, attacks that exploit push fatigue (MFA bombing), reverse phishing proxies, man-in-the-middle (MitM) can defeat most MFA methods.

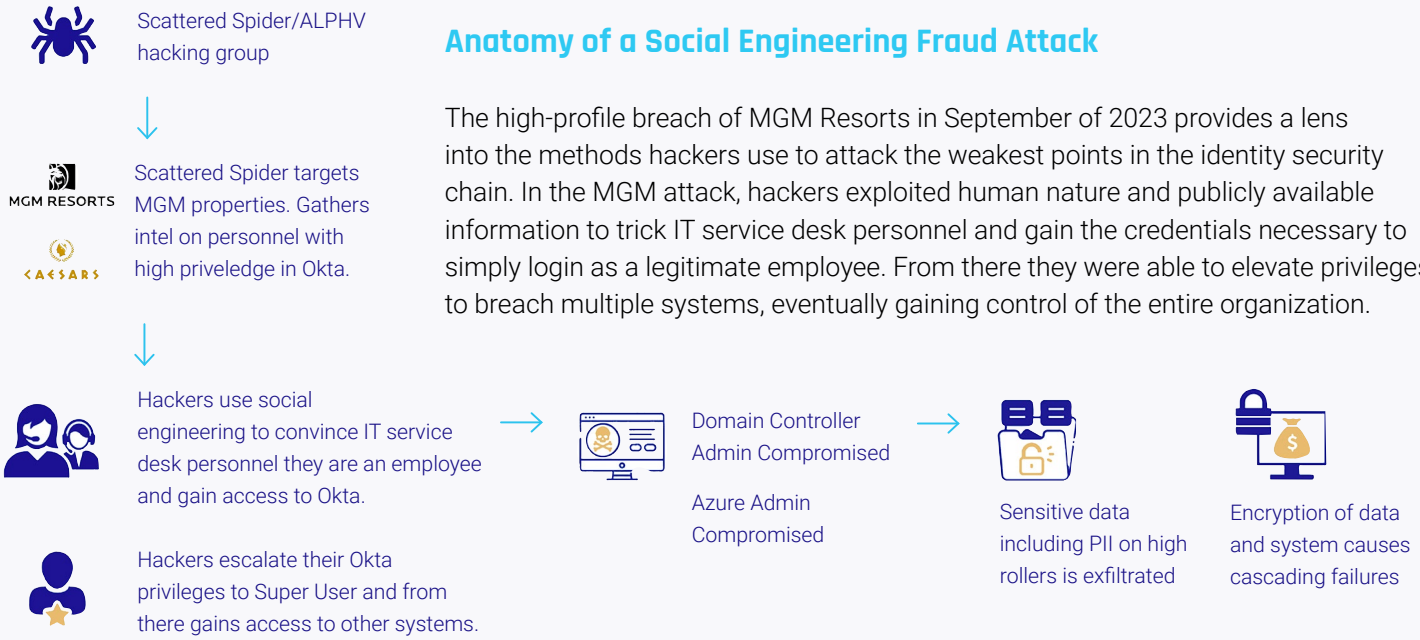
The evident crisis has prompted tighter regulations and greater consequences for violations. The Cybersecurity and Infrastructure Security Agency (CISA) has been advocating for the use of phishing-resistant MFA since early 2022. Other regulatory bodies are quickly catching up — PCI DSS 4.0, goes into effect early 2024, bringing strict password restrictions and multi-factor authentication requirements, with stiff fines for non-compliance.

Increasing Interview fraud

The shift to remote and hybrid work brought an unexpected new threat vector: candidate fraud. Using deepfakes and stolen PII, applicants are impersonating real, qualified individuals, using stand-ins for interviews or other techniques such as voice feeds. Without the means to verify candidates' identities, organizations have no way to ensure that the person they interviewed is the same person they actually hired.

Anatomy of a Social Engineering Fraud Attack

The high-profile breach of MGM Resorts in September of 2023 provides a lens into the methods hackers use to attack the weakest points in the identity security chain. In the MGM attack, hackers exploited human nature and publicly available information to trick IT service desk personnel and gain the credentials necessary to simply login as a legitimate employee. From there they were able to elevate privileges to breach multiple systems, eventually gaining control of the entire organization.



Identity Challenges Abound

Our research shows that all organizations still struggle when it comes to securing their workers' identities. **The top pain point, cited by 40%, is employee identity proofing/verification.** Many organizations use a series of manual processes that are disconnected from their primary identity systems. This has major consequences for security, UX and productivity, as detailed later in this report.

Authentication comes in at a close second challenge, with 37% admitting that their authentication processes are vulnerable to phishing and credential attacks. Extensive investigation into this topic published in the 2023 State of Passwordless Security report suggests that the number is much higher. That research revealed that 97% of the purportedly passwordless solutions include the use of at least one technique that requires a password, shared secret or other phishable technique.

Other top challenges include implementing continuous risk assessment and reducing authentication application sprawl, both named by 35% of organizations.

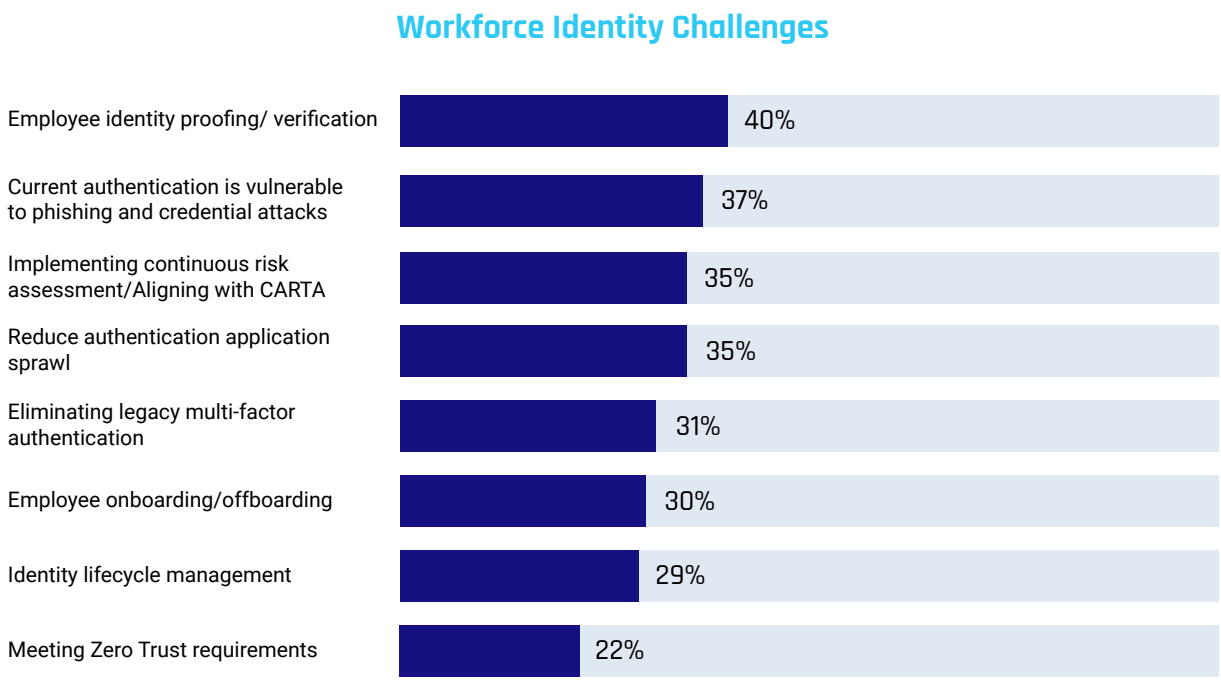


Figure 1: What are the primary identity challenges facing your organization? [100], omitting some answer options

Organizations Contend With Frequent Identity Risks

The findings show that employees engage in risky activities on a regular basis. Around seven in ten organizations (71%) report detecting risky user behavior or unexpected changes in the risk environment multiple times each week; nearly a quarter experience daily risks.

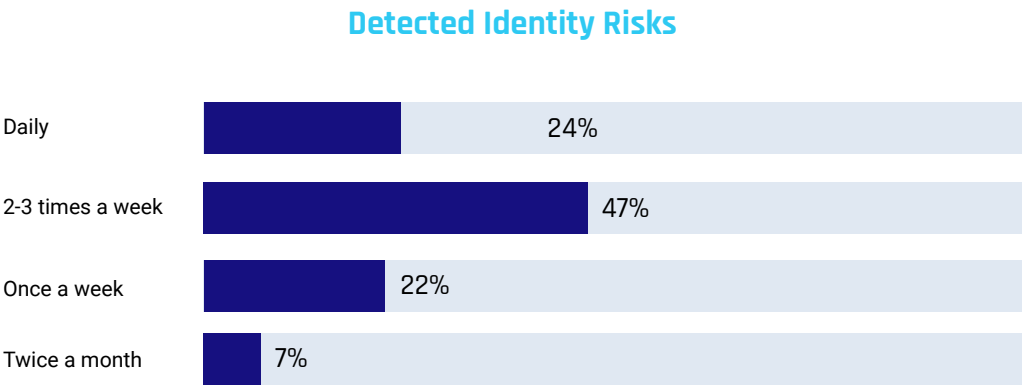


Figure 2: How often does your organization detect risky user behavior or unexpected changes in the risk environment? [100], omitting some answer options

But That's Not the Whole Picture...

In all likelihood, these risk figures skew much higher. Organizations admit their visibility into identity risks remains incomplete. On average, they monitor fewer than half (49%) of their employees' identities on a daily basis for risk or indications of compromise. This potentially leaves a large swath taking risky actions that go undetected.

49% of employee identities are monitored for risk or IOCs daily

Organizations Find It Difficult To Verify Employees in Real Time

With employee identity proofing/verification the top cited pain point, it's hardly surprising that workplaces find real-time verification challenging. The startling part is the amount of time wasted and the breadth of the problem. More than two-thirds of organizations spend over two hours performing employee verification checks when an employee needs to replace a device, when a risk is flagged by security systems or when employees change roles. In some cases the average time spent is much higher. For example it takes an average of 8.52 hours to verify identity when an employee changes roles. This suggests that the vast majority of organizations lack a coherent, optimized approach when it comes to workforce identity verification.

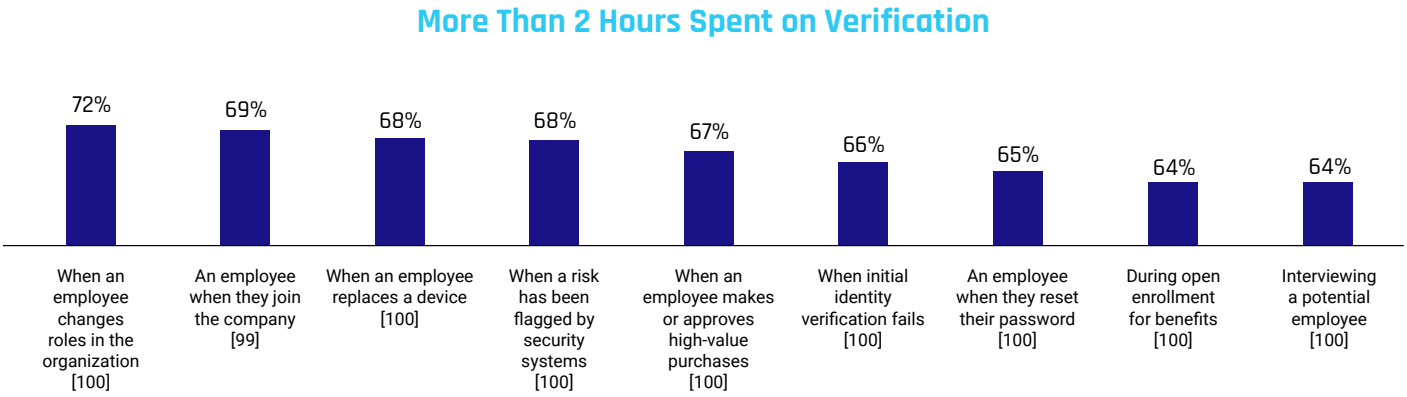


Figure 3: How long does it take for your organization to verify an employee in the following circumstances? [base size in chart], respondents only saw the scenarios that their organization uses verification for

8.52 hours

spent verifying identity when an employee changes roles

7.71 hours

spent verifying identity when an employee replaces a device

Disconnect Between Level of Identity Risk and Confidence

Despite these identified challenges, nearly all (96%) display high levels of confidence in the ability of their organization's identity security tools to prevent a breach. This suggests a misplaced sense of confidence in their current systems or perhaps a willingness to accept elevated levels of risk.

As we will see in the next section, these same organizations admit to confirmed cases of identity fraud, making this contradiction even more glaring. It will be interesting to see if these figures change as stricter regulations come online.

Perceptions of Current Identity Security Tools

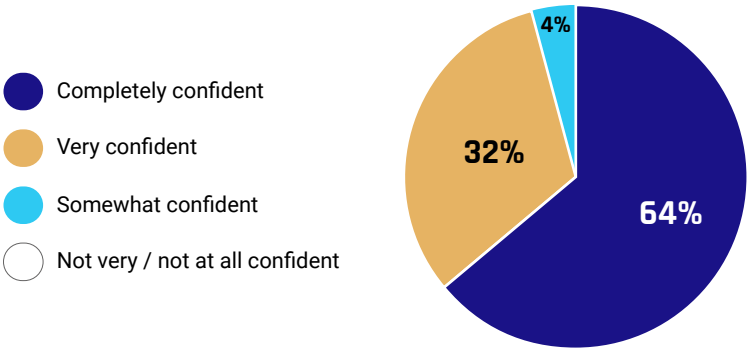


Figure 4: How confident are you in your organization's identity security tools to successfully monitor employee identity risks or indications of compromise such that they can prevent a breach? [100] only asked to those from organizations that monitor their employees' identities

Key Cybersecurity Compliance Deadlines Taking Effect in 2024

Regulation	Deadline	
Payment Card Industry Data Security Standard version 4.0 (PCI DSS 4.0)	March 31	The first phase of PCI DSS 4.0 includes 13 new requirements that companies need to comply with by March 31, 2024.
FTC Safeguards Rule	May 13	New FTC data breach reporting rules for non-banking financial institutions take effect
New State Data Privacy Rules: Florida, Oregon and Texas Montana	July 1 October 1	More states are following California's example and introducing data privacy regulations. These vary in rigor and which companies they apply to.
OMB Zero Trust Guidelines	September 30	Federal agencies have until Sept. 30 to complete 19 specific tasks set out in the OMB memorandum including enforcement of MFA. These requirements may also have implications for organizations that work with the government.

Identity Fraud Is Rampant...

The widespread reliance on insecure identity security solutions is leaving the door wide open to security threats, with undeniable consequences. Identity fraud is so prolific among organizations that over three quarters (77%) report falling victim multiple times within the last 12 months. On average, organizations have been the victim of identity fraud five times in that past year.

Frequency of Identity Fraud in the Last 12 Months

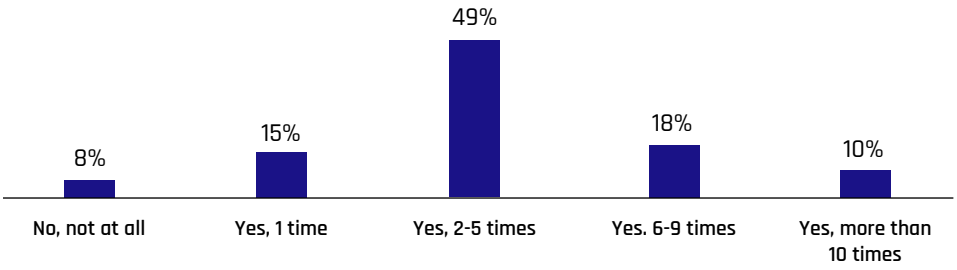


Figure 5: In the last 12 months has your organization been the victim of identity fraud? [100], omitting some answers

... and Costly

On average, identity fraud costs organizations a sizable $4.33 million in the last 12 months. This amount would include the direct expenses of identity fraud, such as regulatory fines, legal costs and investigation costs. However, it's unlikely the financial impact of identity fraud will have stopped there. Longer-term repercussions include reputational damage, downstream breaches, and lost trust and business.

$4.33 M average cost of identity fraud in the last 12 months

Conclusion

These findings reveal the growing fault lines in workplace identity systems and the very real consequences. Insecure authentication practices, patchy identity monitoring and disconnected identity verification processes are leading to operational headaches and widespread identity fraud. Real-time verification of employee identities, in particular, poses a major challenge for organizations, exacerbated by the now-mainstream remote and hybrid work model.

This fragmented identity landscape provides a fertile ground for attackers. Unlike software and hardware exploit attacks, identity threats take advantage of the same systems and processes used by legitimate users. Identity security, therefore, becomes about ensuring the digital identities used to access systems are always tied to a legitimate, verified, real-life identity. This will require organizations to re-examine their current systems, with an eye toward securing the full employee identity lifecycle in an integrated fashion.

Defining New Standards

Industry giants Microsoft, Google, Apple and others have come together with the FIDO Alliance and the World Wide Web Consortium (W3C) to define common identity standards and protocols. Passkey-based authentication already promises to mitigate a large swath of identity security risks. Working groups within these standards bodies are starting to tackle identity verification issues. Emerging trends point to a convergence in identity security protocols, moving toward a more holistic approach.

Comprehensive Identity Assurance

HYPR unites phishing-resistant passwordless authentication, continuous risk orchestration and enhanced identity verification into a comprehensive Identity Assurance solution. With HYPR, you can detect, prevent, and eliminate identity-related risks at every point in the identity lifecycle, ensuring your workforce are who they claim to be at all times while improving their user experience.

Research methodology

HYPR commissioned independent market research agency Vanson Bourne to conduct this research piece. The study surveyed 100 US IT security decision makers who were familiar with their organization's identity and access management solutions during October 2023.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit vansonbourne.com

About HYPR

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments, including 2 of the 4 largest US banks, manufacturers, leading critical infrastructure companies and other technology-forward businesses. HYPR's solutions have been independently validated to return a 324% ROI.

HYPR

THE IDENTITY ASSURANCE COMPANY

www.hypr.com | hypr.com/contact